National Cybersecurity Center of Excellence

Mitigating IoT-Based DDoS

Current State and Next Steps

April 10, 2019

NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Engagement & Business Model

DEFINE

OUTCOME:
Define a scope of work with industry to solve a pressing cybersecurity challenge

ASSEMBLE

OUTCOME:
Assemble teams of industry orgs, govt agencies, and academic institutions to address all aspects of the cybersecurity challenge

BUILD

OUTCOME:
Build a practical, usable, repeatable implementation to address the cybersecurity challenge

ADVOCATE

OUTCOME:
Advocate adoption of the example implementation using the practice guide

Practice Guide Special Publication Series 1800

Typically published as three volumes:

- Volume A: Overview and Executive Summary
  - Audience: CEOs/CIOs
- Volume B: Approach, Architecture, and Security Characteristics
  - Audience: CISOs, Business Owners
- Volume C: How-To Guide – Step-by-Step Configuration
  - Audience: Technical Staff, Implementers and Operators

Current State

DEFINE

OUTCOME:
Define a scope of work with industry to solve a pressing cybersecurity challenge

ASSEMBLE

OUTCOME:
Assemble teams of industry orgs, govt agencies, and academic institutions to address all aspects of the cybersecurity challenge

BUILD

OUTCOME:
Build a practical, usable, repeatable implementation to address the cybersecurity challenge

ADVOCATE

OUTCOME:
Advocate adoption of the example implementation using the practice guide

Build Phases

BUILD 1

- Cisco:
  - MUD Manager/FreeRADIUS
  - Catalyst Switch
- Molex:
  - MUD Capable IoT devices
- DigiCert:
  - Certificates
- ForeScout:
  - CounterAct and Enterprise Mgr.
- NCCoE:
  - IoT devices, MUD File Server, MUD File, Update Server, Unapproved Server

BUILD 2

- MasterPeace:
  - Yikes! Router/MUD Manager
  - Yikes! Cloud
  - Yikes! Mobile App
  - MUD File Server
- DigiCert:
  - Certificates
- NCCoE:
  - IoT devices, MUD File, Update Server, Unapproved Server

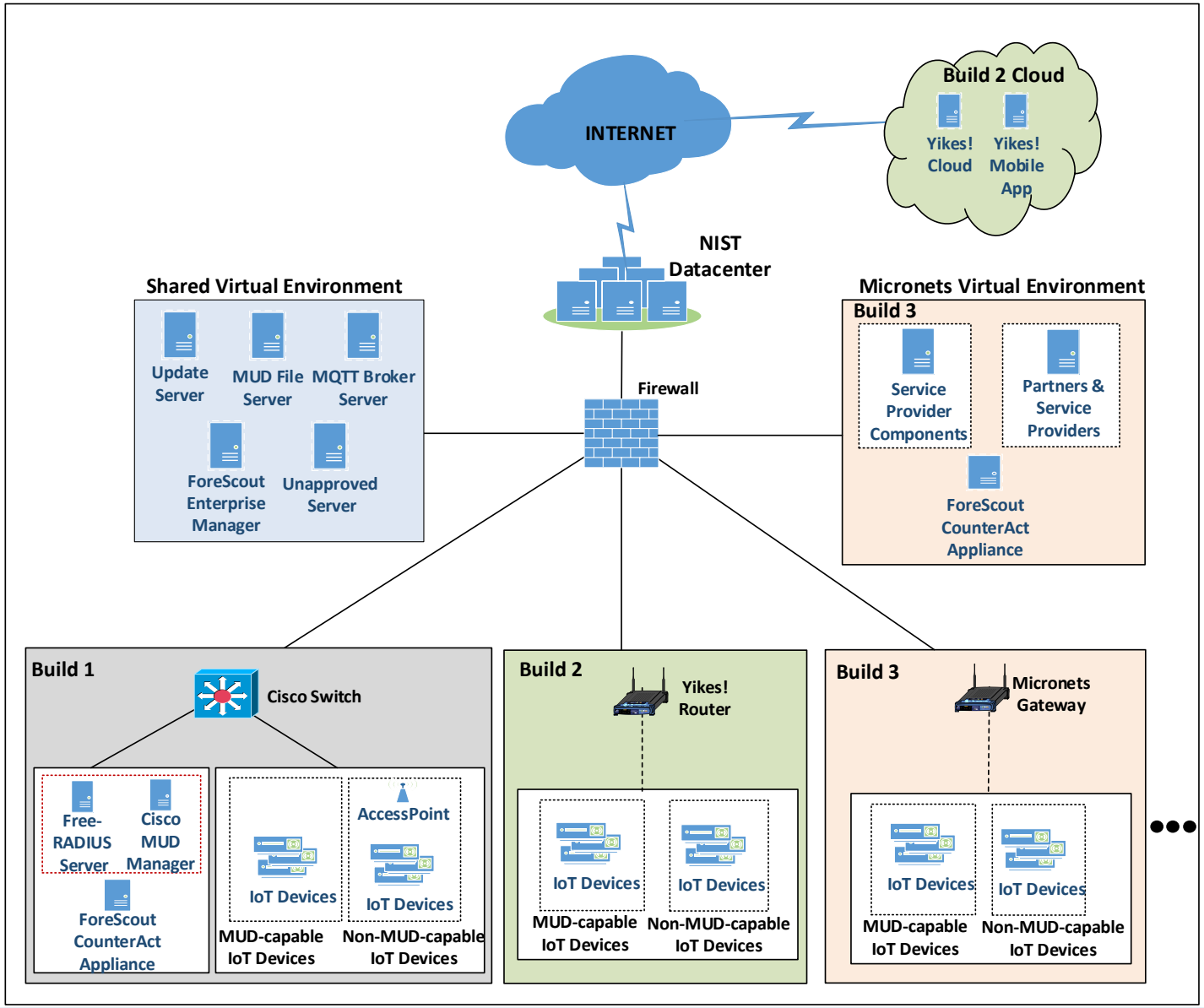
BUILD 3

- CableLabs:
  - Micronets Components, MUD Manager, MUD File Server
  - Micronets Gateway
- DigiCert:
  - Certificates
- NCCoE:
  - IoT devices, MUD File, Update Server, Unapproved Server

Q2 2019

Q4 2019

Lab Architecture



Next Steps

- **Build 1:**
  - Publish Preliminary Draft of Practice Guides Volume A, B and C – Q2 2019
- **Build 2 and 3:**
  - Complete lab setup, integration and testing
  - Publish Draft Practice Guides Volume A, B and C – Q4 2019
- **May have additional Builds based on Collaborators' contribution**
- **Advocate MUD adoption by device manufacturers**
- **Advocate MUD adoption for home and small business use**

NCCoE Team Contact Info

For all communications, please submit to:

mitigating-iot-ddos-nccoe@nist.gov

Questions